Location Verification Systems Under Spatially Correlated Shadowing

Shihao Yan, Ido Nevat, Gareth W. Peters, and Robert Malaney

***Abstract*—The verification of the location information utilized in wireless communication networks is a subject of growing importance. In this work we formally analyze, for the first time, the performance of a wireless Location Verification System (LVS) under the realistic setting of spatially correlated shadowing. Our analysis illustrates that anticipated levels of correlated shadowing can lead to a dramatic performance improvement of a Received Signal Strength (RSS)-based LVS. We also analyze the performance of an LVS that utilizes Differential Received Signal Strength (DRSS), formally proving the rather counter-intuitive result that a DRSS-based LVS has identical performance to that of an RSS-based LVS, for all levels of correlated shadowing. Even more surprisingly, the identical performance of RSS and DRSS-based LVSs is found to hold even when the adversary does not optimize his true location. Only in the case where the adversary does not optimize *all* variables under her control, do we find the performance of an RSS-based LVS to be better than a DRSS-based LVS. The results reported here are important for a wide range of emerging wireless communication applications whose proper functioning depends on the authenticity of the location information reported by a transceiver.**

***Index Terms*—Location verification, wireless networks, Received Signal Strength (RSS), Differential Received Signal Strength (DRSS), spatially correlated shadowing.**

I. Introduction

As location information becomes of growing importance in wireless networks, procedures to formally authenticate (verify) that information have attracted considerable research interest [1–10]. In a wide range of emerging wireless networks, the system may request a device (user) to report its location obtained through some independent means (e.g., via a Global Positioning System (GPS) receiver embedded in the device). Such location information can be used to empower some functionalities or services of wireless networks, such as geographic routing protocols (e.g., [11–13]), location-based access control protocols (e.g., [14, 15]), and location-based services (e.g., location-based key generation [16]). However, the use of location information as an enabler of functionality or services within the wireless network, also provides ample opportunity to attack the system since any reported location information can be easily spoofed. Such potential attacks are perhaps most concerning in the context of emerging Intelligent Transport Systems (ITS) such as vehicular ad hoc networks (VANETs), where spoofed positions may lead to catastrophic results for vehicular collision-avoidance systems [18].

In this work, we focus on a formal analysis of LVSs that attempt to verify a user's claimed location (such as a GPS location) based on independent observations received by the wireless communications network itself. The inference in such an LVS is carried out to determine whether the claimed location represents a *legitimate user* (a user who reports/claims to the network a location *consistent* with his true position) or a *malicious user* (a user who reports to the network a location *inconsistent* with his true position). A key difference between an LVS and a localization system is that the output of an LVS is a binary decision (legitimate/malicious user), whereas in localization system the output is an estimated location (e.g., [19–21]). As such, an LVS is provided with some additional *a priori* (but potentially false) location information (i.e., a claimed location).

Since the RSS measured by wireless network is easily obtained, many location verification algorithms that utilize RSS as input observations have been developed (e.g., [3, 5, 6, 9, 10]). In addition, RSS can be readily combined with other location information metrics in order to improve the performance of a localization system [22, 23]. However, shadowing is one of the most influential factors in RSS-based LVSs, and all existing studies in RSS-based LVSs have made a simplified but unrealistic assumption that the shadowing at two different locations is uncorrelated. As per many empirical studies, the shadowing at different locations will be significantly correlated when the locations are close to each other or different locations possess similar terrain configurations (e.g., [24–26]). Although some specific studies have investigated the performance of RSS-based localization systems under correlated shadowing [27–29], the impact of spatially correlated shadowing on RSS-based LVSs under realistic threat models has not been previously explored. This leaves an important gap in our understanding on the performance levels of RSS-based LVSs in realistic wireless channel settings and under realistic threat models. The main purpose of this paper is to close this gap.

Further to our considerations of RSS-based LVSs, we note that there could be circumstances where the use of Differential Received Signal Strength (DRSS) in the LVS context may be beneficial. Indeed it is well known that there are a range of scenarios in which the use of DRSS is more suitable for wireless location acquisition [30]. One example is where users do not have a common transmit power. However, the

S. Yan was with the School of Electrical Engineering and Telecommunications, The University of New South Wales, Sydney, NSW, Australia. He is currently with the Research School of Engineering, Australia National University, Canberra, ACT, Australia (email: shihao.yan@anu.edu.au).

R. Malaney is with the School of Electrical Engineering and Telecommunications, The University of New South Wales, Sydney, NSW, Australia (email: r.malaney@unsw.edu.au).

I. Nevat is with Institute for Infocomm Research, A*STAR, Singapore (email: ido-nevat@i2r.a-star.edu.sg).

G. W. Peters is with the Department of Statistical Science, University College London, London, United Kingdom (email: gareth.peters@ucl.ac.uk).

Part of this work has been presented in IEEE ICC 2014 [17].

performance of DRSS-based LVSs have not yet been analyzed in the literature. This work also closes this gap, extending our analysis of DRSS-based LVSs to the correlated shadowing regime. This will allow us to provide a detailed performance comparison between RSS-based LVSs and DRSS-based LVSs under correlated shadowing - a comparison that provides for a few surprising results.

A summary of the main contributions of this work are as follows. (i) Under spatially correlated log-normal shadowing, we analyze the detection performance of an RSS-based LVS in terms of false positive and detection rates. Our analysis demonstrates that the spatial correlation of the shadowing can lead to a significant performance improvement for the RSS-based LVS relative to the case with uncorrelated shadowing (a doubling of the detection rate for a given false positive rate for anticipated correlation levels). (ii) We analyze the detection performance of a DRSS-based LVS under spatially correlated shadowing, proving that the detection performance of the DRSS-based LVS is identical to that of the RSS-based LVS. As we discuss later, this result is rather surprising. (iii) We analyze our systems under a relaxed threat model scenario in which the adversary whose actual location is physically constrained (e.g., constrained within a building) and therefore cannot optimize his location for the attack. We show that even in these circumstances the performances of the RSS-based LVS and the DRSS-based LVS remain identical. (iv) Finally, we illustrate the case where the RSS-based LVS do have advantages over the DRSS-Based LVS, namely, when the adversary does not (or cannot) optimize his boosted transmit power level.

The rest of this paper is organized as follows. Section II details our system model. In Section III, the detection performance of the RSS-based LVS is analyzed under spatially correlated shadowing. In Section IV, the detection performance of the DRSS-based LVS is analyzed, and a throughout performance comparison between the RSS-based LVS and the DRSS-based LVS is provided. Section V provides numerical results to verify the accuracy of our analysis. Finally, Section VII draws concluding remarks.

II. System Model

A. Assumptions

We outline the system model and state the assumptions adopted in this work.

1) A *single* user (legitimate or malicious) reports his claimed location, $\mathbf{x}_c = [x_c^1, x_c^2] \in \mathbb{R}^2$, to a network with N Base Stations (BSs) in the communication range of the user, where the publicly known location of the i-th BS is $\mathbf{x}_i = [x_i^1, x_i^2] \in \mathbb{R}^2$ $(i = 1, 2, \ldots, N)$. Any one of the N BSs can be chosen as the Process Center (PC), and all other BSs will transmit the measurements collected from the user to the PC.
2) The user (legitimate or malicious) can obtain his true position, $\mathbf{x}_t = [x_t^1, x_t^2]$, from his localization equipment (e.g., GPS), and the localization error is zero. Thus, a legitimate user's claimed location, $\mathbf{x}_c$, is exactly the same as his true location. However, a malicious user will falsify (spoof) his claimed position in an attempt to fool the LVS. We assume the spoofed claimed location of the malicious user is also $\mathbf{x}_c$.
3) We adopt the minimum distance model as our threat model, in which the distance between the malicious user's true location and his claimed location is greater or equal to r, i.e., $\|\mathbf{x}_c - \mathbf{x}_t\| \geq r$. In this work, we assume the value of r is known to the PC as *a priori* information. In practice, there are three main methods to assign the value of r. The first method is an assignment based on the network operator's view of how close an attacker can be to his claimed location whilst having no fear of physical apprehension (see later discussion in Section VI). A second method could be one dictated by the physical environment. For example, it could be that the threat model is based on a stationary attacker positioned off the highway, and the physical environment (e.g., a fence) dictates he must be a minimum distance from the highway [31–33]. A third method is to set the value of r based on the expected localization error (e.g., GPS error) of a legitimate user. In this case, r would be set so as to guarantee a low probability that the legitimate user's true location is outside the region determined by $\mathbf{x}_c$ and r. A combination (e.g., weighted value) of all methods could also be used.
4) We denote the null hypothesis where the user is legitimate as $\mathcal{H}_0$, and denote the alternative hypothesis where the user is malicious as $\mathcal{H}_1$. The *a priori* knowledge at the LVS can be summarized as

$$\begin{cases} \mathcal{H}_0: \ \mathbf{x}_c = \mathbf{x}_t \ \text{(legitimate user)}, \\ \mathcal{H}_1: \ \|\mathbf{x}_c - \mathbf{x}_t\| \geq r \ \text{(malicious user)}. \end{cases} \tag{1}$$

B. Observation Model under $\mathcal{H}_0$

Based on the log-normal propagation model, the RSS (in dB) received by the i-th BS from a legitimate user, y_i, is given by

$$y_i = u_i + \omega_i, \quad i = 1, 2, \ldots, N, \tag{2}$$

where

$$u_i = p - 10\gamma \log_{10}\left(\frac{d_i^c}{d}\right), \tag{3}$$

and p is a reference received power corresponding to a reference distance d, γ is the path loss exponent, ω_i is a zero-mean normal random variable with variance σ_{dB}^2, and d_i^c is the Euclidean distance from the i-th BS to the legitimate user's claimed location (also his true location) given by $d_i^c = \|\mathbf{x}_c - \mathbf{x}_i\|$. We note that $d_i^c = d_i^t$ under $\mathcal{H}_0$, where $d_i^t = \|\mathbf{x}_t - \mathbf{x}_i\|$. In practice, in order to determine the values of p and d we have to know the transmit power of the legitimate user. We highlight that in this work we assume that the transmit power of the legitimate user is known to the LVS. This is mainly due to the fact that the legitimate user cooperates with the LVS in order to facilitate the location verification. To this end, the legitimate user will set his transmit power to a predetermined value set by the LVS. For fairness, we also assume that the malicious user also knows the transmit

power of the legitimate user (equivalently, knows the values of p and d), which allows the malicious user to optimally set his transmit power in order to minimize the probability to be detected. Under spatially correlated shadowing, ω_i is correlated to ω_j ($j = 1, 2, \ldots, N$), and the $N \times N$ covariance matrix of $\boldsymbol{\omega} = [\omega_1, \ldots, \omega_N]$ is denoted as $\mathbf{R}$. Adopting the well-known spatially correlated shadowing model of [7, 24], the (i, j)-th element of $\mathbf{R}$ is given by

$$R_{ij} = \sigma_{dB}^2 \exp\left(-\frac{d_{ij}}{D_c} \ln 2\right), \quad j = 1, 2, \ldots, N, \tag{4}$$

where $d_{ij} = \|\mathbf{x}_i - \mathbf{x}_j\|$ is the Euclidean distance from the i-th BS to the j-th BS and D_c is a constant in units of distance, at which the correlation coefficient reduces to $1/2$ (in this work all distances are in meters). From (4), we can see that the correlation between ω_i and ω_j decreases as d_{ij} increases ($R_{ij} = \sigma_{dB}^2$ when $i = j$, and $R_{ij} \to 0$ as $d_{ij} \to \infty$). We also note that R_{ij} increases as D_c increases for a given d_{ij}. As such, D_c is a parameter that indicates the degree of shadowing correlation in some specific environment (for a given d_{ij}, a larger D_c means that the shadowing is more correlated).

Based on (2), we can see that under $\mathcal{H}_0$ the N-dimensional observation vector $\mathbf{y} = [y_1, \ldots, y_N]^T$ follows a multivariate normal distribution, which is

$$f(\mathbf{y}|\mathcal{H}_0) = \mathcal{N}(\mathbf{u}, \mathbf{R}), \tag{5}$$

where $\mathbf{u} = [u_1, u_2, \ldots, u_N]^T$ is the mean vector.

C. Observation Model under $\mathcal{H}_1$

In practice, in addition to spoofing the claimed location, the malicious user can also adjust his transmit power to impact the RSS values received by all BSs in order to minimize the probability of being detected. As such, the RSS received by the i-th BS from a malicious user, y_i, is given by

$$y_i = p_x + v_i + \omega_i, \tag{6}$$

where

$$v_i = p - 10\gamma \log_{10}\left(\frac{d_i^t}{d}\right), \tag{7}$$

and p_x is the additional boosted transmit power. We note that p_x is the same for all the BSs since the additional transmit power only effects the value of p and the distance between i-th BS and the malicious user is absorbed by v_i. Based on (6), under $\mathcal{H}_1$ the N-dimensional observation vector $\mathbf{y}$, conditioned on known p_x and $\mathbf{x}_t$, also follows a multivariate normal distribution, which is

$$f(\mathbf{y}|p_x, \mathbf{x}_t, \mathcal{H}_1) = \mathcal{N}(p_x \mathbf{1}_N + \mathbf{v}, \mathbf{R}), \tag{8}$$

where $\mathbf{1_N}$ is a $N \times 1$ vector with all elements set to unity and $\mathbf{v} = [v_1, v_2, \ldots, v_N]^T$. We note that in practice p_x and $\mathbf{x}_t$ are set by the malicious user.

D. Decision Rule of an LVS

We adopt the Likelihood Ratio Test (LRT) as the decision rule since it is optimal for binary hypothesis testing problem in terms of achieving the highest detection rate for any given false positive rate [34]. Therefore, the LRT can achieve the minimum Bayesain average cost [35] and the maximum mutual information between the input and output of an LVS [10]. Given that no related work on LVSs under correlated shadowing is available in the literature, in this work we focus on analyzing the detection performances of our LVSs rather than comparisons with other works. We note that the deployment of the LRT requires that the likelihood functions under both $\mathcal{H}_0$ and $\mathcal{H}_1$ can be evaluated exactly in analytic forms (i.e., there are no nuisance parameters involved in these likelihood functions). In general, the likelihood function under $\mathcal{H}_1$ is dependent on some parameters (e.g., p_x, $\mathbf{x}_t$) that are unknown to the LVS. In this work we adopt a conservative scenario, in which we assume that the malicious user can optimize all the parameters under his control. We refer to this scenario as the worst-case scenario throughout this work. In practice, if the malicious user cannot optimize all the parameters under his control, our analysis based on the worst-case scenario serves as the lower bound for the detection performance of a practical LVS. The LRT decision rule is given by

$$\Lambda(\psi(\mathbf{y})) \triangleq \frac{f(\psi(\mathbf{y})|\mathcal{H}_1)}{f(\psi(\mathbf{y})|\mathcal{H}_0)} \underset{\mathcal{D}_0}{\overset{\mathcal{D}_1}{\gtrless}} \lambda, \tag{9}$$

where $\Lambda(\psi(\mathbf{y}))$ is the test statistic, $\psi(\mathbf{y})$ is a predefined transformation of $\mathbf{y}$, $f(\psi(\mathbf{y})|\mathcal{H}_1)$ is the likelihood function (probability density function of $\psi(\mathbf{y})$) under $\mathcal{H}_1$, $f(\psi(\mathbf{y})|\mathcal{H}_0)$ is the likelihood function under $\mathcal{H}_0$, λ is the threshold corresponding to $\Lambda(\psi(\mathbf{y}))$, $\mathcal{D}_0$ and $\mathcal{D}_1$ are the binary decisions that infer whether the user is legitimate or malicious, respectively. It is worth noting that another definition of the likelihood ratio (e.g., composite likelihood ratio) has to be adopted if some parameters under $\mathcal{H}_0$ and $\mathcal{H}_1$ are unknown. In our work, (9) does not involve any unknown parameters based on the worst-case scenario. We clarify that in our RSS-based LVS we have $\psi(\mathbf{y}) = \mathbf{y}$, i.e., no transformation function is utilized in the RSS-based LVS. In our DRSS-based LVS the transformation function $\psi(\cdot)$ maps the RSS into DRSS (detailed in Section IV-A). Although $\psi(\mathbf{y})$ in our work is still normal given that $\mathbf{y}$ is normal, $\psi(\mathbf{y})$ is not necessarily normal since the transformation may be not linear. Given the decision rule in (9), the false positive and detection rates of an LVS are functions of λ. The intrinsic core performance metrics of an LVS are false positive and detection rates, other potential performance metrics can be written as functions of these two rates. As such, in this work we adopt the false positive and detection rates as the performance metrics for an LVS. We note that *a priori* probabilities may be required for some performance metrics adopted by an LVS. For example, the Bayesian average cost is defined as $C = P_0 \alpha C_0 + (1 - P_0)(1 - \beta) C_1$, where P_0 is the *a priori* probability that $\mathcal{H}_0$ is true, C_0 is the pre-assigned cost of rejecting a legitimate user, and C_1 is the pre-assigned cost of accepting a malicious user [35]. We highlight that in

order to achieve the overall minimum Bayesian average cost the likelihood ratio (i.e., $\Lambda(\psi(\mathbf{y}))$) should be adopted as the test statistic.

III. RSS-based Location Verification System

In this section, we analyze the performance of the RSS-based LVS in terms of the false positive and detection rates, based on which we examine the impact of the spatially correlated shadowing.

A. Attack Strategy of the Malicious User

We assume that the malicious user optimizes all the parameters under his control. This assumption is adopted in most threat models. The ultimate goal of the malicious user is to minimize the detection rate. To this end, the malicious user is to minimize the KL divergence from $f(\mathbf{y}|p_x, \mathbf{x}_t, \mathcal{H}_1)$ to $f(\mathbf{y}|\mathcal{H}_0)$ [36]. This result is mainly due to the fact that the threshold λ and observation $\mathbf{y}$ are unknown to the malicious user and the KL divergence from $f(\mathbf{y}|p_x, \mathbf{x}_t, \mathcal{H}_1)$ to $f(\mathbf{y}|\mathcal{H}_0)$ is the expected log likelihood ratio when the alternative hypothesis $\mathcal{H}_1$ is true.

Based on (5) and (8), the KL divergence from $f(\mathbf{y}|p_x, \mathbf{x}_t, \mathcal{H}_1)$ to $f(\mathbf{y}|\mathcal{H}_0)$ is given by [37]

$$\begin{aligned}\phi(p_x, \mathbf{x}_t) &= D_{KL}\left[f(\mathbf{y}|p_x, \mathbf{x}_t, \mathcal{H}_1)\,||\,f(\mathbf{y}|\mathcal{H}_0)\right] \\ &= \int_{-\infty}^{\infty} \ln \frac{f(\mathbf{y}|p_x, \mathbf{x}_t, \mathcal{H}_1)}{f(\mathbf{y}|\mathcal{H}_0)} f(\mathbf{y}|p_x, \mathbf{x}_t, \mathcal{H}_1)\, d\mathbf{y} \\ &= \frac{1}{2}(p_x\mathbf{1}_N + \mathbf{v} - \mathbf{u})^T\mathbf{R}^{-1}(p_x\mathbf{1}_N + \mathbf{v} - \mathbf{u}). \quad (10)\end{aligned}$$

Then, the optimal values of p_x and $\mathbf{x}_t$ that minimize $\phi(p_x, \mathbf{x}_t)$ can be obtained through

$$(p_x^*, \mathbf{x}_t^*) = \underset{p_x, \|\mathbf{x}_t - \mathbf{x}_c\| \geq r}{\operatorname{argmin}} \phi(p_x, \mathbf{x}_t). \quad (11)$$

The closed-form expressions for p_x^* and $\mathbf{x}_t^*$ are intractable, but they can be obtained through numerical search. In order to simplify the numerical search, we first derive the optimal value of p_x for a given $\mathbf{x}_t$, which is presented in the following lemma.

Lemma 1: The optimal value of p_x that minimizes $\phi(p_x, \mathbf{x}_t)$ for any given $\mathbf{x}_t$ is

$$p_x^o(\mathbf{x}_t) = \frac{(\mathbf{u} - \mathbf{v})^T\mathbf{R}^{-1}\mathbf{1}_N}{\mathbf{1}_N^T\mathbf{R}^{-1}\mathbf{1}_N}. \quad (12)$$

Proof: The first derivative of $\phi(p_x, \mathbf{x}_t)$ with respect to p_x is derived as

$$\begin{aligned}\frac{\partial\phi(p_x, \mathbf{x}_t)}{\partial p_x} &= \frac{\partial\phi(p_x, \mathbf{x}_t)}{\partial(p_x\mathbf{1}_N)} \frac{\partial(p_x\mathbf{1}_N)}{\partial p_x} \\ &= (p_x\mathbf{1}_N + \mathbf{v} - \mathbf{u})^T\mathbf{R}^{-1}\frac{\partial(p_x\mathbf{1}_N)}{\partial p_x} \\ &= (p_x\mathbf{1}_N + \mathbf{v} - \mathbf{u})^T\mathbf{R}^{-1}\mathbf{1}_N. \quad (13)\end{aligned}$$

Following (13), the second derivative of $\phi(p_x, \mathbf{x}_t)$ with respect to p_x is derived as

$$\frac{\partial^2\phi(p_x, \mathbf{x}_t)}{\partial^2 p_x} = \mathbf{1}_N^T\mathbf{R}^{-1}\mathbf{1}_N. \quad (14)$$

Noting that $\mathbf{R}$ given by (4) is a positive-definite matrix, as per (14) we have $\partial^2\phi(p_x, \mathbf{x}_t)/\partial^2 p_x > 0$, which indicates that $\phi(p_x, \mathbf{x}_t)$ is a convex function of p_x. As such, setting $\partial\phi(p_x, \mathbf{x}_t)/\partial p_x = 0$, we obtain the desired result in (12) after some algebraic manipulations. ■

From Lemma 1, we note that the malicious user optimizes his transmit power, i.e., $p_x = p_x^o(\mathbf{x}_t)$, to compensate the path-loss difference between his claimed location and his true location. We also note that $p_x^o(\mathbf{x}_t)$ is a function of $\mathbf{R}$ under spatial correlated shadowing. This is different from the scenario with uncorrelated shadowing, where $p_x^o(\mathbf{x}_t)$ is independent of the shadowing noise [10]. Substituting $p_x^o(\mathbf{x}_t)$ into (10), we have

$$\phi(p_x^o(\mathbf{x}_t), \mathbf{x}_t) = \frac{1}{2}(\mathbf{w} - \mathbf{u})^T\mathbf{R}^{-1}(\mathbf{w} - \mathbf{u}), \quad (15)$$

where

$$\mathbf{w} = \frac{(\mathbf{u} - \mathbf{v})^T\mathbf{R}^{-1}\mathbf{1}_N}{\mathbf{1}_N^T\mathbf{R}^{-1}\mathbf{1}_N}\mathbf{1}_N + \mathbf{v}. \quad (16)$$

Since we have shown that $\phi(p_x, \mathbf{x}_t)$ is a convex function of p_x in (14), $\mathbf{x}_t^*$ can be obtained through

$$\mathbf{x}_t^* = \underset{\|\mathbf{x}_t - \mathbf{x}_c\| \geq r}{\operatorname{argmin}} \phi(p_x^o(\mathbf{x}_t), \mathbf{x}_t). \quad (17)$$

Substituting $\mathbf{x}_t^*$ into $p_x^o(\mathbf{x}_t)$, we obtain $p_x^* = p_x^o(\mathbf{x}_t^*)$. We note that Lemma 1 is of importance since it reduces a three-dimension numerical search in (11) into a two-dimension numerical search in (17). On average, the computing time required to search for $\mathbf{x}_t^*$ in (17) is around 20 seconds when the grid search method is adopted and 100 points in each dimension are searched (based on MATLAB R2014b on a DELL desktop with a Core i7 processor).

Substituting p_x^* and $\mathbf{x}_t^*$ into (6), the RSS received by the i-th BS from a malicious user can be written as

$$\mathbf{y} = \mathbf{w}^* + \boldsymbol{\omega}, \quad (18)$$

where

$$\mathbf{w}^* = \frac{(\mathbf{u} - \mathbf{v}^*)^T\mathbf{R}^{-1}\mathbf{1}_N}{\mathbf{1}_N^T\mathbf{R}^{-1}\mathbf{1}_N}\mathbf{1}_N + \mathbf{v}*, \quad (19)$$

$\mathbf{v}^*$ is obtained by substituting $\mathbf{x}_t^*$ into $\mathbf{v}$. Based on (18), the likelihood function under $\mathcal{H}_1$ conditioned on p_x^* and $\mathbf{x}_t^*$ can be written as

$$f(\mathbf{y}|p_x^*, \mathbf{x}_t^*, \mathcal{H}_1) = \mathcal{N}(\mathbf{w}^*, \mathbf{R}). \quad (20)$$

B. Performance of the RSS-based LVS

In some practical cases, the malicious user may not have the freedom to optimize his true location, e.g., the malicious user is physically limited to be inside a building. However, the malicious user can still optimize his transmit power as per his true location. As such, without losing generality, we first analyze the performance of the RSS-based LVS for $p_x = p_x^o(\mathbf{x}_t)$, and then present the performance of the RSS-based LVS for $p_x = p_x^*$ and $\mathbf{x}_t = \mathbf{x}_t^*$ as a special case.

Following (9) and noting $\psi(\mathbf{y}) = \mathbf{y}$, the specific LRT decision rule of the RSS-based LVS for $p_x = p_x^o(\mathbf{x}_t)$ is given by

$$\Lambda^o(\mathbf{y}) \triangleq \frac{f(\mathbf{y}|p_x^o(\mathbf{x}_t), \mathbf{x}_t, \mathcal{H}_1)}{f(\mathbf{y}|\mathcal{H}_0)} \underset{\mathcal{D}_0}{\overset{\mathcal{D}_1}{\gtrless}} \lambda_R^o, \tag{21}$$

where $\Lambda^o(\mathbf{y})$ is the likelihood ratio of $\mathbf{y}$ for $p_x = p_x^o(\mathbf{x}_t)$, $f(\mathbf{y}|p_x^o(\mathbf{x}_t), \mathbf{x}_t, \mathcal{H}_1) = \mathcal{N}(\mathbf{w}, \mathbf{R})$, and λ_R^o is a threshold for $\Lambda^o(\mathbf{y})$. Then, we obtain $\Lambda^o(\mathbf{y})$ in the $\ln$ domain as

$$\begin{aligned}\ln \Lambda^o(\mathbf{y}) &= \frac{1}{2}(\mathbf{y}-\mathbf{u})^T \mathbf{R}^{-1}(\mathbf{y}-\mathbf{u}) - \frac{1}{2}(\mathbf{y}-\mathbf{w})^T \mathbf{R}^{-1}(\mathbf{y}-\mathbf{w}) \\ &= (\mathbf{w}-\mathbf{u})^T \mathbf{R}^{-1}\mathbf{y} - \frac{1}{2}(\mathbf{w}-\mathbf{u})^T \mathbf{R}^{-1}(\mathbf{w}+\mathbf{u}).\end{aligned}$$

As such, for the theorem to follow, we can rewrite the decision rule in (21) as the following format

$$\mathbb{T}(\mathbf{y}) \underset{\mathcal{D}_0}{\overset{\mathcal{D}_1}{\gtrless}} \Gamma_R, \tag{22}$$

where $\mathbb{T}(\mathbf{y})$ is the test statistic given by

$$\mathbb{T}(\mathbf{y}) \triangleq (\mathbf{w}-\mathbf{u})^T \mathbf{R}^{-1}\mathbf{y}, \tag{23}$$

and Γ_R is the threshold for $\mathbb{T}(\mathbf{y})$ given by

$$\Gamma_R \triangleq \ln \lambda_R^o + \frac{1}{2}(\mathbf{w}-\mathbf{u})^T \mathbf{R}^{-1}(\mathbf{w}+\mathbf{u}). \tag{24}$$

We note that (22) is the explicit binary decision rule at the PC for the RSS-based LVS. In (22) only the test statistic $\mathbb{T}(\mathbf{y})$ is a function of the observations. The threshold Γ_R can be determined by setting an acceptable false positive rate, minimizing the Bayesian average cost, or maximizing the mutual information between the input and output of the RSS-based LVS. To this end, we have to derive the false positive rate, α_R^o, and detection rate, β_R^o, of the RSS-based LVS, which are provided in the following theorem.

Theorem 1: For $p_x = p_x^o(\mathbf{x}_t)$, the false positive and detection rates of the RSS-based LVS are

$$\begin{aligned}\alpha_R^o(\mathbf{x}_t) &= \mathcal{Q}\left[\frac{\Gamma_R - (\mathbf{w}-\mathbf{u})^T \mathbf{R}^{-1}\mathbf{u}}{\sqrt{(\mathbf{w}-\mathbf{u})^T \mathbf{R}^{-1}(\mathbf{w}-\mathbf{u})}}\right] \\ &= \mathcal{Q}\left[\frac{\ln \lambda_R^o + \frac{1}{2}(\mathbf{w}-\mathbf{u})^T \mathbf{R}^{-1}(\mathbf{w}-\mathbf{u})}{\sqrt{(\mathbf{w}-\mathbf{u})^T \mathbf{R}^{-1}(\mathbf{w}-\mathbf{u})}}\right],\end{aligned} \tag{25}$$

$$\begin{aligned}\beta_R^o(\mathbf{x}_t) &= \mathcal{Q}\left[\frac{\Gamma_R - (\mathbf{w}-\mathbf{u})^T \mathbf{R}^{-1}\mathbf{w}}{\sqrt{(\mathbf{w}-\mathbf{u})^T \mathbf{R}^{-1}(\mathbf{w}-\mathbf{u})}}\right] \\ &= \mathcal{Q}\left[\frac{\ln \lambda_R^o - \frac{1}{2}(\mathbf{w}-\mathbf{u})^T \mathbf{R}^{-1}(\mathbf{w}-\mathbf{u})}{\sqrt{(\mathbf{w}-\mathbf{u})^T \mathbf{R}^{-1}(\mathbf{w}-\mathbf{u})}}\right],\end{aligned} \tag{26}$$

where $\mathcal{Q}[x] = \frac{1}{\sqrt{2\pi}} \int_x^\infty \exp(-t^2/2)dt$.

Proof: Using (23), the distributions of $\mathbb{T}(\mathbf{y})$ under $\mathcal{H}_0$ and $\mathcal{H}_1$ are derived as follows

$$\mathbb{T}(\mathbf{y})|\mathcal{H}_0 \sim \mathcal{N}\left((\mathbf{w}-\mathbf{u})^T \mathbf{R}^{-1}\mathbf{u}, (\mathbf{w}-\mathbf{u})^T \mathbf{R}^{-1}(\mathbf{w}-\mathbf{u})\right), \tag{27}$$

$$\mathbb{T}(\mathbf{y})|\mathcal{H}_1 \sim \mathcal{N}\left((\mathbf{w}-\mathbf{u})^T \mathbf{R}^{-1}\mathbf{w}, (\mathbf{w}-\mathbf{u})^T \mathbf{R}^{-1}(\mathbf{w}-\mathbf{u})\right). \tag{28}$$

As per the decision rule in (22), the false positive and detection rates are given by

$$\alpha_R^o(\mathbf{x}_t) \triangleq \Pr\left(\mathbb{T}(\mathbf{y}) \geq \Gamma_R|\mathcal{H}_0\right), \tag{29}$$

$$\beta_R^o(\mathbf{x}_t) \triangleq \Pr\left(\mathbb{T}(\mathbf{y}) \geq \Gamma_R|\mathcal{H}_1\right). \tag{30}$$

Substituting (27) and (28) into (29) and (30), respectively, we obtain the results in (25) and (26) after some algebraic manipulations. ■

For $p_x = p_x^*$ and $\mathbf{x}_t = \mathbf{x}_t^*$, the LRT decision rule of the RSS-based LVS is given by

$$\Lambda^*(\mathbf{y}) \triangleq \frac{f(\mathbf{y}|p_x^*, \mathbf{x}_t^*, \mathcal{H}_1)}{f(\mathbf{y}|\mathcal{H}_0)} \underset{\mathcal{D}_0}{\overset{\mathcal{D}_1}{\gtrless}} \lambda_R^*, \tag{31}$$

where $\Lambda^*(\mathbf{y})$ is the likelihood ratio of $\mathbf{y}$ for $p_x = p_x^*$ and $\mathbf{x}_t = \mathbf{x}_t^*$, and λ_R^* is a threshold for $\Lambda^*(\mathbf{y})$. Following Theorem 1, the false positive and detection rates of the RSS-based LVS for $p_x = p_x^*$ and $\mathbf{x}_t = \mathbf{x}_t^*$ are given by

$$\alpha_R^* = \mathcal{Q}\left[\frac{\ln \lambda_R^* + \frac{1}{2}(\mathbf{w}^*-\mathbf{u})^T \mathbf{R}^{-1}(\mathbf{w}^*-\mathbf{u})}{\sqrt{(\mathbf{w}^*-\mathbf{u})^T \mathbf{R}^{-1}(\mathbf{w}^*-\mathbf{u})}}\right], \tag{32}$$

$$\beta_R^* = \mathcal{Q}\left[\frac{\ln \lambda_R^* - \frac{1}{2}(\mathbf{w}^*-\mathbf{u})^T \mathbf{R}^{-1}(\mathbf{w}^*-\mathbf{u})}{\sqrt{(\mathbf{w}^*-\mathbf{u})^T \mathbf{R}^{-1}(\mathbf{w}^*-\mathbf{u})}}\right]. \tag{33}$$

We note that the results provided in (25) and (26) are based on an arbitrary true location $\mathbf{x}_t$ of the malicious user, which are more general than that provided in (32) and (33). That is, $\alpha_R^* = \alpha_R^o(\mathbf{x}_t^*)$ and $\beta_R^* = \beta_R^o(\mathbf{x}_t^*)$. By using (25) and (26), we can compare the performance of the RSS-based LVS with that of the DRSS-based LVS in a general scenario. We also note that based on (32) and (33) we can examine the impact of shadowing correlation on the detection performance of the RSS-based LVS. Considering the properties of the $\mathcal{Q}$-function, we have the following corollary.

Corollary 1: The detection performance of the RSS-based LVS increases as $\kappa \triangleq (\mathbf{w}^*-\mathbf{u})^T \mathbf{R}^{-1}(\mathbf{w}^*-\mathbf{u})$ increases, i.e., β_R^* increases for any fixed α_R^* as κ increases (or α_R^* decreases for any fixed β_R^* as κ increases).

Proof: Let us suppose we have two LVSs, LVS-1 and LVS-2. We assume that the false positive rate and detection rate of LVS-k ($k \in \{1, 2\}$) are given by, respectively,

$$\alpha_k = \mathcal{Q}\left[\frac{\ln \lambda_k + \frac{1}{2}\kappa_k}{\sqrt{\kappa_k}}\right] = \mathcal{Q}\left[\frac{\ln \lambda_k}{\sqrt{\kappa_k}} + \frac{\sqrt{\kappa_k}}{2}\right], \tag{34}$$

$$\beta_k = \mathcal{Q}\left[\frac{\ln \lambda_k - \frac{1}{2}\kappa_k}{\sqrt{\kappa_k}}\right] = \mathcal{Q}\left[\frac{\ln \lambda_k}{\sqrt{\kappa_k}} - \frac{\sqrt{\kappa_k}}{2}\right]. \tag{35}$$

We note that $\mathcal{Q}[x]$ is a monotonic decreasing function of x. Then, following (34) and setting $\alpha_1 = \alpha_2$, we have

$$\frac{\ln \lambda_1}{\sqrt{\kappa_1}} + \frac{\sqrt{\kappa_1}}{2} = \frac{\ln \lambda_2}{\sqrt{\kappa_2}} + \frac{\sqrt{\kappa_2}}{2}. \tag{36}$$

Suppose $\kappa_1 < \kappa_2$, by subtracting $\sqrt{\kappa_1}$ and $\sqrt{\kappa_2}$ from the left side and right side of (36), respectively, we have

$$\frac{\ln \lambda_1}{\sqrt{\kappa_1}} - \frac{\sqrt{\kappa_1}}{2} > \frac{\ln \lambda_2}{\sqrt{\kappa_2}} - \frac{\sqrt{\kappa_2}}{2}. \tag{37}$$

As such, following (35) and (37) we have $\beta_1 < \beta_2$. Therefore, we have proved that $\beta_1 < \beta_2$ for $\alpha_1 = \alpha_2$ if $\kappa_1 < \kappa_2$. Similarly, we can prove that $\alpha_1 > \alpha_2$ for $\beta_1 = \beta_2$ if $\kappa_1 < \kappa_2$. Comparing (32) and (33) with (34) and (35), respectively, the proof follows. ∎

Corollary 1 is consistent with our previous conclusion that the malicious user will minimize the KL-divergence given in (10) in order to minimize the detection performance of an LVS, because $\frac{1}{2}\left(\mathbf{w}^*-\mathbf{u}\right)^T \mathbf{R}^{-1}\left(\mathbf{w}^*-\mathbf{u}\right)$ is the minimum value of the KL-divergence given in (15). Therefore, in order to examine the impact of the shadowing correlation we only have to check whether an increased correlation (e.g., increased D_c) leads to an increased or decreased value of $\frac{1}{2}\left(\mathbf{w}^*-\mathbf{u}\right)^T \mathbf{R}^{-1}\left(\mathbf{w}^*-\mathbf{u}\right)$. Due to the fact that $\mathbf{x}_t^*$ cannot be obtained analytically, it is impossible to theoretically analyze the impact of shadowing correlation on the detection performance of the RSS-based LVS. In this regard, we will examine this impact numerically. As we will show in Section V the correlation of the shadowing leads to performance improvements in practical scenarios. Intuitively, this is due to the fact that the shadowing correlation reduces the uncertainty of the observations caused by shadowing noise, and consequently it becomes harder for the malicious user to mimic these observations. Following Corollary 1, we have the following corollary with regard to how the values of σ_{dB}^2 effect the performance of the RSS-based LVS.

Corollary 2: The detection rate of the RSS-based LVS decreases as σ_{dB}^2 increases for any arbitrary fixed false positive rate (or the false positive rate of the RSS-based LVS increases as σ_{dB}^2 increases for any arbitrary fixed detection rate).

Following Corollary 1, we can prove Corollary 2 by noting that κ decreases as σ_{dB}^2 increases due to (4).

IV. DRSS-based Location Verification System

In this section, we analyze the detection performance of the DRSS-based LVS under spatially correlated shadowing. We also provide an analytical comparison between the RSS-based LVS and the DRSS-based LVS.

A. DRSS Observations

We obtain $(N-1)$ basic DRSS observations from N RSS observations by subtracting the N-th RSS observation from all other $(N-1)$ RSS observations. As such, the m-th DRSS value under $\mathcal{H}_0$ is given by

$$\Delta y_m = \Delta u_m + \Delta\omega_m, \quad m = 1, 2, \ldots, N-1, \tag{38}$$

where $\Delta u_m = u_m - u_N$ and $\Delta\omega_m = \omega_m - \omega_N$. We note that $\Delta\omega_m$ is Gaussian with zero mean and variance $2(\sigma_{dB}^2 - R_{mN})$. We denote the $(N-1)\times(N-1)$ covariance matrix of the $(N-1)$-dimensional DRSS vector $\mathbf{\Delta y} = [\Delta y_1, \ldots, \Delta y_{N-1}]^T$ as $\mathbf{D}$, whose (m,n)-th element is given by $(n = 1, 2, \ldots, N-1)$

$$D_{mn} = R_{NN} + R_{mn} - R_{mN} - R_{nN}. \tag{39}$$

As such, $\mathbf{\Delta y}$ under $\mathcal{H}_0$ follows a multivariate normal distribution, which is given by

$$f\left(\mathbf{\Delta y}|\mathcal{H}_0\right) = \mathcal{N}(\mathbf{\Delta u}, \mathbf{D}), \tag{40}$$

where $\mathbf{\Delta u} = [\Delta u_1, \ldots, \Delta u_{N-1}]^T$ is the mean vector.

Likewise, the m-th DRSS value under $\mathcal{H}_1$ is

$$\Delta y_m = \Delta v_m + \Delta\omega_m, \tag{41}$$

where $\Delta v_m = v_m - v_N$. Noting $\mathbf{\Delta v} = [\Delta v_1, \ldots, \Delta v_{N-1}]^T$, $\mathbf{\Delta y}$ under $\mathcal{H}_1$ follows another multivariate normal distribution, which is given by

$$f\left(\mathbf{\Delta y}|\mathbf{x}_t, \mathcal{H}_1\right) = \mathcal{N}(\mathbf{\Delta v}, \mathbf{D}). \tag{42}$$

B. Attack Strategy of the Malicious User

As per (3) and (7), we know that both p and d are constant at all elements of $\mathbf{u}$ and $\mathbf{v}$. As such, based on (38) and (41) we can see that $\mathbf{\Delta y}$ under both $\mathcal{H}_0$ and $\mathcal{H}_1$ is independent of p and d, and therefore both $f\left(\mathbf{\Delta y}|\mathcal{H}_0\right)$ and $f\left(\mathbf{\Delta y}|\mathbf{x}_t, \mathcal{H}_1\right)$ are independent of p and d. As such, in the DRSS-based LVS the malicious user does not need to adjust his transmit power in order to minimize the detection rate. In the DRSS-based LVS, the malicious user only has to optimize his true location through minimizing the KL-divergence from $f\left(\mathbf{\Delta y}|\mathbf{x}_t, \mathcal{H}_1\right)$ to $f\left(\mathbf{\Delta y}|\mathcal{H}_0\right)$, which is given by

$$\begin{aligned}\varphi(\mathbf{x}_t) &= D_{KL}\left[f\left(\mathbf{\Delta y}|\mathbf{x}_t, \mathcal{H}_1\right)||f\left(\mathbf{\Delta y}|\mathcal{H}_0\right)\right] \\ &= \int_{-\infty}^{\infty} \ln\frac{f\left(\mathbf{\Delta y}|\mathbf{x}_t, \mathcal{H}_1\right)}{f\left(\mathbf{\Delta y}|\mathcal{H}_0\right)} f\left(\mathbf{\Delta y}|\mathbf{x}_t, \mathcal{H}_1\right) d\mathbf{\Delta y} \\ &= \frac{1}{2}(\mathbf{\Delta v} - \mathbf{\Delta u})^T \mathbf{D}^{-1}(\mathbf{\Delta v} - \mathbf{\Delta u}).\end{aligned} \tag{43}$$

Then, the optimal value of $\mathbf{x}_t$ for the malicious user in the DRSS-based LVS can be obtained through

$$\mathbf{x}_t^\dagger = \underset{\|\mathbf{x}_t - \mathbf{x}_c\| \geq r}{\operatorname{argmin}} \varphi(\mathbf{x}_t). \tag{44}$$

The likelihood function under $\mathcal{H}_1$ for $\mathbf{x}_t = \mathbf{x}_t^\dagger$ is given by

$$f\left(\mathbf{\Delta y}|\mathbf{x}_t^\dagger, \mathcal{H}_1\right) = \mathcal{N}(\mathbf{\Delta v}^\dagger, \mathbf{D}), \tag{45}$$

where $\Delta v_m^\dagger = v_m^\dagger - v_N^\dagger$ and $\mathbf{v}^\dagger$ is obtained by substituting $\mathbf{x}_t^\dagger$ into $\mathbf{v}$.

C. Performance of the DRSS-based LVS

In this subsection, we again consider the case where the true location of the malicious user is physically constrained. Specifically, we first analyze the performance of the DRSS-based LVS for an arbitrary $\mathbf{x}_t$, and then present the performance of the DRSS-based LVS for $\mathbf{x}_t = \mathbf{x}_t^\dagger$ as a special case in this subsection.

Following (9), the specific LRT decision rule of the DRSS-based LVS for any $\mathbf{x}_t$ is given by

$$\Lambda\left(\mathbf{\Delta y}\right) \triangleq \frac{f\left(\mathbf{\Delta y}|\mathbf{x}_t, \mathcal{H}_1\right)}{f\left(\mathbf{\Delta y}|\mathcal{H}_0\right)} \underset{\mathcal{D}_0}{\overset{\mathcal{D}_1}{\gtrless}} \lambda_D, \tag{46}$$

where $\Lambda\left(\mathbf{\Delta y}\right)$ is the likelihood ratio of $\mathbf{\Delta y}$ and λ_D is a threshold for $\Lambda\left(\mathbf{\Delta y}\right)$. Substituting (40) and (45) into (46),

we obtain $\Lambda(\mathbf{\Delta y})$ in $\ln$ domain as

$$\begin{aligned}\ln\Lambda(\mathbf{\Delta y}) &= \frac{1}{2}(\mathbf{\Delta y}-\mathbf{\Delta u})^T\mathbf{D}^{-1}(\mathbf{\Delta y}-\mathbf{\Delta u}) \\ &\quad -\frac{1}{2}(\mathbf{\Delta y}-\mathbf{\Delta v})^T\mathbf{D}^{-1}(\mathbf{\Delta y}-\mathbf{\Delta v}) \\ &= (\mathbf{\Delta v}-\mathbf{\Delta u})^T\mathbf{D}^{-1}\mathbf{\Delta y} \\ &\quad -\frac{1}{2}(\mathbf{\Delta v}-\mathbf{\Delta u})^T\mathbf{D}^{-1}(\mathbf{\Delta v}+\mathbf{\Delta u}).\end{aligned}$$

Then, we can rewrite the decision rule given in (46) as

$$\mathbb{T}(\mathbf{\Delta y}) \underset{\mathcal{D}_1}{\overset{\mathcal{D}_0}{\gtrless}} \Gamma_D, \tag{47}$$

where $\mathbb{T}(\mathbf{\Delta y})$ is the test statistic given by

$$\mathbb{T}(\mathbf{\Delta y}) \triangleq (\mathbf{\Delta v}-\mathbf{\Delta u})^T\mathbf{D}^{-1}\mathbf{\Delta y}, \tag{48}$$

and Γ_D is the threshold for $\mathbb{T}(\mathbf{\Delta y})$ given by

$$\Gamma_D \triangleq \ln\lambda_D + \frac{1}{2}(\mathbf{\Delta v}-\mathbf{\Delta u})^T\mathbf{D}^{-1}(\mathbf{\Delta v}+\mathbf{\Delta u}). \tag{49}$$

We would like to highlight that (47) is the explicit binary decision rule at the PC for the DRSS-based LVS. In (47) only the test statistic $\mathbb{T}(\mathbf{\Delta y})$ depends on the DRSS observations $\mathbf{\Delta y}$. The threshold Γ_D can be determined by setting an acceptable false positive rate, minimizing the Bayesian average cost, or maximizing the mutual information between the input and output of the DRSS-based LVS. In this regard, the false positive rate, $\alpha_D(\mathbf{x}_t)$, and the detection rate, $\beta_D(\mathbf{x}_t)$, of the DRSS-based LVS have to be derived, which are present in the following theorem.

Theorem 2: The false positive and detection rates of the DRSS-based LVS for any $\mathbf{x}_t$ are given by

$$\begin{aligned}\alpha_D(\mathbf{x}_t) &= \mathcal{Q}\left[\frac{\Gamma_D-(\mathbf{\Delta v}-\mathbf{\Delta u})^T\mathbf{D}^{-1}\mathbf{\Delta u}}{\sqrt{(\mathbf{\Delta v}-\mathbf{\Delta u})^T\mathbf{D}^{-1}(\mathbf{\Delta v}-\mathbf{\Delta u})}}\right] \\ &= \mathcal{Q}\left[\frac{\ln\lambda_D+\frac{1}{2}(\mathbf{\Delta v}-\mathbf{\Delta u})^T\mathbf{D}^{-1}(\mathbf{\Delta v}-\mathbf{\Delta u})}{\sqrt{(\mathbf{\Delta v}-\mathbf{\Delta u})^T\mathbf{D}^{-1}(\mathbf{\Delta v}-\mathbf{\Delta u})}}\right],\end{aligned} \tag{50}$$

$$\begin{aligned}\beta_D(\mathbf{x}_t) &= \mathcal{Q}\left[\frac{\Gamma_D-(\mathbf{\Delta v}-\mathbf{\Delta u})^T\mathbf{D}^{-1}\mathbf{\Delta v}}{\sqrt{(\mathbf{\Delta v}-\mathbf{\Delta u})^T\mathbf{D}^{-1}(\mathbf{\Delta v}-\mathbf{\Delta u})}}\right] \\ &= \mathcal{Q}\left[\frac{\ln\lambda_D-\frac{1}{2}(\mathbf{\Delta v}-\mathbf{\Delta u})^T\mathbf{D}^{-1}(\mathbf{\Delta v}-\mathbf{\Delta u})}{\sqrt{(\mathbf{\Delta v}-\mathbf{\Delta u})^T\mathbf{D}^{-1}(\mathbf{\Delta v}-\mathbf{\Delta u})}}\right].\end{aligned} \tag{51}$$

The proof of Theorem 2 is similar to that of Theorem 1 and omitted here due to page limits.

For $\mathbf{x}_t=\mathbf{x}_t^\dagger$, the LRT decision rule of the DRSS-based LVS is given by

$$\Lambda^*(\mathbf{\Delta y}) \triangleq \frac{f(\mathbf{\Delta y}|\mathbf{x}_t,\mathcal{H}_1)}{f(\mathbf{\Delta y}|\mathcal{H}_0)} \underset{\mathcal{D}_0}{\overset{\mathcal{D}_1}{\gtrless}} \lambda_D^*, \tag{52}$$

where $\Lambda^*(\mathbf{\Delta y})$ is the likelihood ratio of $\mathbf{\Delta y}$ for $\mathbf{x}_t=\mathbf{x}_t^\dagger$ and λ_D^* is a threshold for $\Lambda^*(\mathbf{\Delta y})$. Following Theorem 2, the false positive and detection rates of the DRSS-based LVS for $\mathbf{x}_t=\mathbf{x}_t^\dagger$ are given by

$$\alpha_D^* = \mathcal{Q}\left[\frac{\ln\lambda_D^*+\frac{1}{2}\left(\mathbf{\Delta v}^\dagger-\mathbf{\Delta u}\right)^T\mathbf{D}^{-1}\left(\mathbf{\Delta v}^\dagger-\mathbf{\Delta u}\right)}{\sqrt{\left(\mathbf{\Delta v}^\dagger-\mathbf{\Delta u}\right)^T\mathbf{D}^{-1}\left(\mathbf{\Delta v}^\dagger-\mathbf{\Delta u}\right)}}\right], \tag{53}$$

$$\beta_D^* = \mathcal{Q}\left[\frac{\ln\lambda_D^*-\frac{1}{2}\left(\mathbf{\Delta v}^\dagger-\mathbf{\Delta u}\right)^T\mathbf{D}^{-1}\left(\mathbf{\Delta v}^\dagger-\mathbf{\Delta u}\right)}{\sqrt{\left(\mathbf{\Delta v}^\dagger-\mathbf{\Delta u}\right)^T\mathbf{D}^{-1}\left(\mathbf{\Delta v}^\dagger-\mathbf{\Delta u}\right)}}\right]. \tag{54}$$

Again, note that the results provided in (50) and (51) are for any $\mathbf{x}_t$, which are more general than that provided in (53) and (54). That is, $\alpha_D^*=\alpha_D(\mathbf{x}_t^\dagger)$ and $\beta_D^*=\beta_D(\mathbf{x}_t^\dagger)$. By using (50) and (51), we can compare the performance of the DRSS-based LVS with that of the RSS-based LVS in a general scenario.

D. Comparison between the RSS-based LVS and the DRSS-based LVS

We now present the following theorem with regard to the comparison between the RSS-based LVS and the DRSS-based LVS.

Theorem 3: For any $\mathbf{x}_t$, we have $\alpha_R^o(\mathbf{x}_t)=\alpha_D(\mathbf{x}_t)$ and $\beta_R^o(\mathbf{x}_t)=\beta_D(\mathbf{x}_t)$ for $\lambda_R=\lambda_D$. That is, for any $\mathbf{x}_t$ the performance of the RSS-based LVS with $p_x=p_x^o(\mathbf{x}_t)$ is identical to the performance of the DRSS-based LVS.

Proof: Based on (25), (26), (50), and (51), we can see that $\alpha_R^o(\mathbf{x}_t)$, $\beta_R^o(\mathbf{x}_t)$, $\alpha_D(\mathbf{x}_t)$, and $\beta_D(\mathbf{x}_t)$ are all in the form of a $\mathcal{Q}$ function. We denote $\alpha_R^o(\mathbf{x}_t)=\mathcal{Q}(\zeta_R^o)$, $\beta_R^o(\mathbf{x}_t)=\mathcal{Q}(\eta_R^o)$, $\alpha_D(\mathbf{x}_t)=\mathcal{Q}(\zeta_D)$, and $\beta_D(\mathbf{x}_t)=\mathcal{Q}(\eta_D)$. In order to prove $\alpha_R^o(\mathbf{x}_t)=\alpha_D(\mathbf{x}_t)$ and $\beta_R^o(\mathbf{x}_t)=\beta_D(\mathbf{x}_t)$ for $\lambda_R=\lambda_D$, we only need to prove $\zeta_R^o-\eta_R^o=\zeta_D-\eta_D$. As per (25), (26), (50), and (51), in order to prove $\zeta_R^o-\eta_R^o=\zeta_D-\eta_D$ (such as to prove Theorem 3) we have to prove the following equation

$$(\mathbf{w}-\mathbf{u})^T\mathbf{R}^{-1}(\mathbf{w}-\mathbf{u}) = (\mathbf{\Delta v}-\mathbf{\Delta u})^T\mathbf{D}^{-1}(\mathbf{\Delta v}-\mathbf{\Delta u}). \tag{55}$$

Based on the singular value decomposition (SVD) of $\mathbf{R}$, we can transform the RSS observation vector $\mathbf{y}$ into another observation vector $\mathbf{y}'$ by rotating and scaling[1]. We can then obtain the DRSS observations from $\mathbf{y}'$ instead of $\mathbf{y}$. The transformation from $\mathbf{y}$ to $\mathbf{y}'$ is unique since the singular values of $\mathbf{R}$ are unique. In addition, $\mathbf{y}$ follows a multivariate normal distribution. As such, the transformation from $\mathbf{y}$ to $\mathbf{y}'$ keeps all the properties of $\mathbf{y}$ in $\mathbf{y}'$, which means the performance of an LVS based on $\mathbf{y}$ is identical to the performance of an LVS based on $\mathbf{y}'$ [38, 39]. Therefore, in order to prove Theorem 3 we only have to prove (55) for $\mathbf{R}=\mathbf{I}_N$. Denoting $\mathbf{g}=\mathbf{v}-\mathbf{u}$, we have $\Delta v_m-\Delta u_m=g_m-g_N$. Substituting $\mathbf{R}=\mathbf{I}_N$ into $\mathbf{w}$ given in (16), we obtain

$$\mathbf{w}-\mathbf{u}=\mathbf{g}-\frac{\mathbf{g}^T\mathbf{R}^{-1}\mathbf{1}_N}{\mathbf{1}_N^T\mathbf{R}^{-1}\mathbf{1}_N}\mathbf{1}_N=\mathbf{g}-\left(\frac{1}{N}\sum_{j=1}^{N}g_j\right)\mathbf{1}_N.$$

[1]The covariance matrix $\mathbf{R}$ is a real positive-definite symmetric matrix, and thus the SVD of $\mathbf{R}$ can be written as $\mathbf{R}=\mathbf{S}\mathbf{R}'\mathbf{S}^T$. As such, $\mathbf{y}'$ is given by $\mathbf{y}'=\mathbf{R}'^{\frac{1}{2}}\mathbf{S}\mathbf{y}$ and the covariance matrix of $\mathbf{y}'$ will be $\mathbf{I}_N$.

With regard to the left side of (55), for $\mathbf{R}=\mathbf{I}_N$ we have

$$\begin{aligned}
&(\mathbf{w}–\mathbf{u})^T\mathbf{R}^{-1}(\mathbf{w}–\mathbf{u}) = \sum_{i=1}^{N}\left(g_i-\frac{1}{N}\sum_{j=1}^{N}g_j\right)^2\\
&=\sum_{i=1}^{N}\left[g_i^2-\frac{2}{N}g_i\sum_{j=1}^{N}g_j+\frac{1}{N^2}\left(\sum_{j=1}^{N}g_j\right)^2\right]\\
&=\left[\sum_{i=1}^{N}g_i^2-\frac{2}{N}\left(\sum_{i=1}^{N}g_i\right)\left(\sum_{j=1}^{N}g_j\right)+\frac{1}{N}\left(\sum_{j=1}^{N}g_j\right)^2\right]\\
&=\left[\sum_{i=1}^{N}g_i^2-\frac{1}{N}\left(\sum_{i=1}^{N}g_i\right)^2\right]. \qquad (56)
\end{aligned}$$

As per the definition of $\mathbf{D}$ given in (39), for $\mathbf{R}=\mathbf{I}_N$ we have

$$\mathbf{D}=\mathbf{I}_{N-1}+\mathbf{1}_{(N-1)\times(N-1)}, \qquad (57)$$

where $\mathbf{1}_{(N-1)\times(N-1)})$ is the $(N-1)\times(N-1)$ matrix with all elements set to unity. Then, based on the Sherman-Morrison formula [40], we have

$$\begin{aligned}
\mathbf{D}^{-1}&=\left[\mathbf{I}_{N-1}+\mathbf{1}_{(N-1)}\times\mathbf{1}_{(N-1)}^T\right]^{-1}\\
&=\left[\mathbf{I}_{N-1}^{-1}-\frac{\mathbf{I}_{N-1}^{-1}\mathbf{1}_{(N-1)\times(N-1)}\mathbf{I}_{N-1}^{-1}}{1+\mathbf{1}_{(N-1)}^T\mathbf{I}_{N-1}^{-1}\mathbf{1}_{(N-1)}}\right]\\
&=\left[\mathbf{I}_{N-1}-\frac{\mathbf{1}_{(N-1)\times(N-1)}}{N}\right]. \qquad (58)
\end{aligned}$$

Substituting (58) into the right side of (55), we have

$$\begin{aligned}
&(\boldsymbol{\Delta}\mathbf{v}–\boldsymbol{\Delta}\mathbf{u})^T\mathbf{D}^{-1}(\boldsymbol{\Delta}\mathbf{v}–\boldsymbol{\Delta}\mathbf{u})\\
&=(\boldsymbol{\Delta}\mathbf{v}–\boldsymbol{\Delta}\mathbf{u})^T\left[\mathbf{I}_{N-1}–\frac{\mathbf{1}_{(N-1)\times(N-1)}}{N}\right](\boldsymbol{\Delta}\mathbf{v}–\boldsymbol{\Delta}\mathbf{u})\\
&=(\boldsymbol{\Delta}\mathbf{v}–\boldsymbol{\Delta}\mathbf{u})^T\mathbf{I}_{N-1}(\boldsymbol{\Delta}\mathbf{v}–\boldsymbol{\Delta}\mathbf{u})\\
&\quad-\frac{1}{N}(\boldsymbol{\Delta}\mathbf{v}–\boldsymbol{\Delta}\mathbf{u})^T\mathbf{1}_{(N-1)}\times\mathbf{1}_{(N-1)}^T(\boldsymbol{\Delta}\mathbf{v}–\boldsymbol{\Delta}\mathbf{u})\\
&=\sum_{i=1}^{N-1}(g_i-g_N)^2-\frac{1}{N}\left[\sum_{i=1}^{N-1}(g_i-g_N)\right]^2\\
&=\sum_{i=1}^{N}(g_i-g_N)^2-\frac{1}{N}\left[\sum_{i=1}^{N}(g_i-g_N)\right]^2\\
&=\sum_{i=1}^{N}(g_i-g_N)^2-\frac{1}{N}\sum_{i=1}^{N}(g_i-g_N)\left[\sum_{j=1}^{N}(g_j-g_N)\right]\\
&=\left[\sum_{i=1}^{N}g_i^2-\frac{1}{N}\left(\sum_{i=1}^{N}g_i\right)^2\right]. \qquad (59)
\end{aligned}$$

Comparing (56) with (59), we can see that we have proved (55) for $\mathbf{R}=\mathbf{I}_N$. This completes the proof of Theorem 3. ■

We note that the result provided in Theorem 3 is valid for any $\mathbf{R}$, i.e., for any kind of shadowing (correlated or uncorrelated). We also note that in Theorem 3 the condition to guarantee the RSS-based LVS being identical to the DRSS-based LVS is that $p_x = p_x^o(\mathbf{x}_t)$. This condition forces the malicious user to optimize his transmit power based on the given $\mathbf{x}_t$ in the RSS-based LVS, but not in the DRSS-based LVS. Without this condition, the comparison result between the RSS-based LVS and the DRSS-based LVS is present in the following corollary. Two intuitive explanations for Theorem 3 are as follows. i) Knowing the transmit power of the legitimate user by the LVS enables the RSS-based LVS to gain an advantage over the DRSS-based LVS. This is due to the fact that p together with d provide useful information on RSS observations while DRSS observations are not functions of p and d. ii) The malicious user's knowledge on p and d allows him to optimally set his transmit power (equivalently, to optimize p_x) in the RSS-based LVS. This nullifies the advantage of the RSS-based LVS over the DRSS-based LVS.

Following Theorem 3, we further have the following four corollaries with regard to the performances of the RSS-based and DRSS-based LVSs.

Corollary 3: For any $N+1>2$ the detection performances of the RSS-based and DRSS-based LVSs will at be at least as good as the performances for N.

The proof of Corollary 3 follows from the fact that the RHS of (56) (and (59)) for $N+1>2$ is equal or larger than that for N. We note that the equality can only occur in the most unusual of circumstances (such as the malicious user reporting his true location). As such, in practice increases in N will effectively always lead to an improvement in detection performance.

Corollary 4: In the DRSS-based LVS, any of the BSs can be selected as the reference BS, and this selection does not effect the performance of the DRSS-based LVS.

The proof of Corollary 4 follows from the fact that (59) does not depend on the selection of the reference BS.

Corollary 5: For any $\mathbf{x}_t$, the performance of the RSS-based LVS with $p_x \neq p_x^o(\mathbf{x}_t)$ is better than the performance of the DRSS-based LVS.

The proof of Corollary 5 follows from Corollary 1 and the proof of Theorem 3.

Corollary 6: We have $\alpha_R^*=\alpha_D^*$ and $\beta_R^*=\beta_D^*$ for $\lambda_R^*=\lambda_D^*$. That is, the performance of the RSS-based LVS for $p_x=p_x^*$ and $\mathbf{x}_t=\mathbf{x}_t^*$ is identical to the performance of the DRSS-based LVS for $\mathbf{x}_t=\mathbf{x}_t^\dagger$.

Proof: Based on Theorem 3, in order to prove Corollary 6 we only have to prove $\mathbf{x}_t^*=\mathbf{x}_t^\dagger$. We note that $\mathbf{x}_t^*$ and $\mathbf{x}_t^\dagger$ are obtained through minimizing $\phi(p_x^o(\mathbf{x}_t),\mathbf{x}_t)$ and $\varphi(\mathbf{x}_t)$, respectively. As such, in order to prove $\mathbf{x}_t^*=\mathbf{x}_t^\dagger$, it suffices to prove $\phi(p_x^o(\mathbf{x}_t),\mathbf{x}_t)=\varphi(\mathbf{x}_t)$. As per (15) and (43), we can see that we have proved $\phi(p_x^o(\mathbf{x}_t),\mathbf{x}_t)=\varphi(\mathbf{x}_t)$ in (55). ■

We note that Corollary 6 presents a comparison between the performance limits of the RSS-based LVS and the DRSS-based LVS. In the proof of Corollary 6, we also prove that the malicious user's optimal true location for the RSS-based LVS is the same as that for the DRSS-based LVS. We also note that the analysis and results reported in this work are not directly applicable to the colluding threat scenario (where multiple colluding adversaries attack the LVS). Future studies may wish to explore these more sophisticated attacks, in the context of correlated shadowing. However, although such sophisticated attacks will obviously lead to poorer LVS performance, a

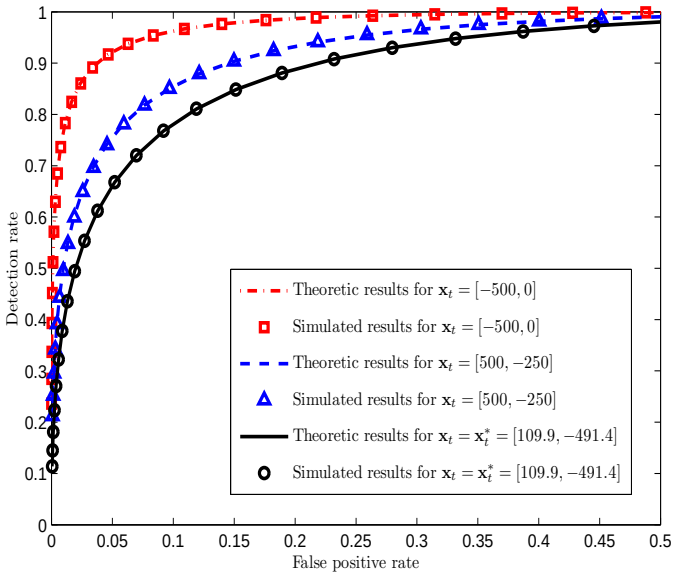

Fig. 1. ROC curves of the RSS-based LVS for $\sigma_{dB} = 7.5$, $D_c = 50$m, $r = 500$m, $p_x = p_x^o(\mathbf{x}_t)$, and $N = 3$ $\big(\mathbf{x}_1 = [-250, 10]$, $\mathbf{x}_2 = [0, -10]$, and $\mathbf{x}_3 = [250, 10]\big)$.

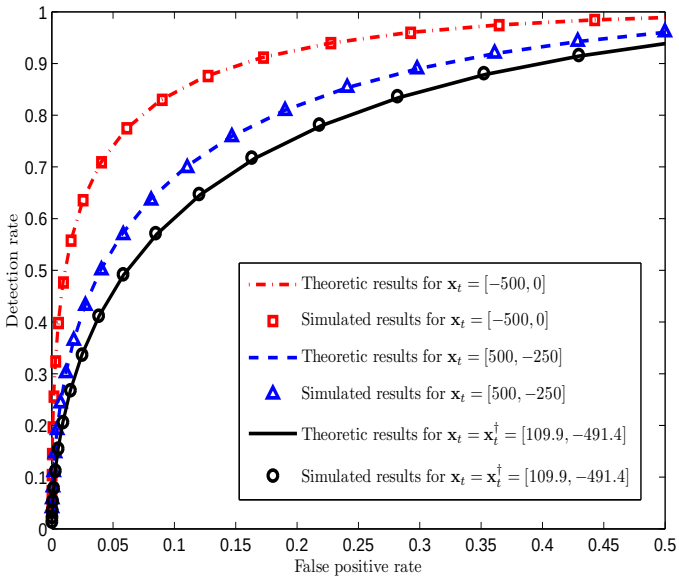

Fig. 2. ROC curves of the DRSS-based LVS for $\sigma_{dB} = 10$, $D_c = 50$m, $r = 500$m, and $N = 3$ $\big(\mathbf{x}_1 = [-250, 10]$, $\mathbf{x}_2 = [0, -10]$, and $\mathbf{x}_3 = [250, 10]\big)$.

conjecture is that the trends discovered here with regard to the impact of correlated shadowing on LVS performance will persist.

V. Numerical Results

We now present numerical results to verify the accuracy of our provided analysis. We also provide some insights on the impact of the spatially correlated shadowing on the performance of the RSS-based LVS and the DRSS-based LVS.

Although we have simulated a wide range of system settings, the associated settings for the results shown in this work (unless otherwise stated) are as follows. In the simulations presented here, the BSs and the claimed locations are deployed in a 500m-by-20m rectangular area and a 200m-by-200m square area. The 500m-by-20m rectangular area mimics a stretch of a road (e.g., a highway) in which emerging ITS will be applicable and LVSs will be of significant importance. The simulations for the 200m-by-200m square area investigates LVSs in the context of wireless sensor networks, in which senors provide observation of various physical phenomena (e.g., temperature, humidity) together with their location information to the BSs. The origin is set at the center of the rectangular area, with the x-coordinate taken along the length, and the y-coordinate taken along the width. The claimed location of a user (legitimate or malicious) is set as $\mathbf{x}_c = [50, 5]$, which is also the true location of the legitimate user. The locations of all BSs are provided in the caption of each figure, and all BSs collect measurements from the legitimate and malicious users. The path loss exponent is set to $\gamma = 3$, and the reference power is set to $p = -10$ dB at $d = 1$m.

In Fig. 1, we present the Receiver Operating Characteristic (ROC) curves of the RSS-based LVS. In order to obtain this figure, we have set the BSs at regular intervals (250m) on each side of the rectangular area. In this figure, we first observe that the Monte Carlo simulations precisely match the theoretic results, confirming our analysis in Theorem 1. We also observe that the ROC curves for $\mathbf{x}_t \neq \mathbf{x}_t^*$ dominate the ROC curve for $\mathbf{x}_t = \mathbf{x}_t^*$. This observation indicates that if the malicious user does not optimize his true location, it will be easier for the RSS-based LVS to detect the malicious user. In summary, the ROC curve for $\mathbf{x}_t = \mathbf{x}_t^*$ provides a lower bound for the performance of the RSS-based LVS.

In Fig. 2, we present the ROC curves of the DRSS-based LVS. In order to obtain this figure, we have adopted the same locations of the BSs. We note that a different value of σ_{dB} is adopted to produce Fig. 2 in order to avoid the identical between Fig. 1 and Fig. 2. In this figure, we first observe that the Monte Carlo simulations precisely match the theoretic results, confirming our analysis in Theorem 2. We also observe that the ROC curves for $\mathbf{x}_t \neq \mathbf{x}_t^\dagger$ dominate the ROC curve for $\mathbf{x}_t = \mathbf{x}_t^\dagger$. Again, this observation demonstrates the importance of optimally choosing the true location for the malicious user. To conclude, the ROC curve for $\mathbf{x}_t = \mathbf{x}_t^\dagger$ provides a lower bound for the performance of the DRSS-based LVS.

In Fig. 3, we present the ROC curves of the RSS-based LVS and the DRSS-based LVS. In order to obtain this figure, we have set one of the BSs at one side of the rectangular area and deployed the other two BSs randomly inside the rectangular area. This mimics the scenario in which only one fixed BS is available and we have to conduct location verification with the help of two already-authorized vehicles. In this figure, we first observe that the RSS-based LVS for $p_x = p_x^o(\mathbf{x}_t)$ and the DRSS-based LVS achieve identical performance (identical ROC curves). This demonstrates that as long as the malicious user optimizes his transmit power (as per his true location) the RSS-based LVS is identical to the DRSS-based LVS, which confirms the analytical comparison between the RSS-based LVS and the DRSS-based LVS presented in Theorem 3. We also observe that the ROC curves of the RSS-based LVS for

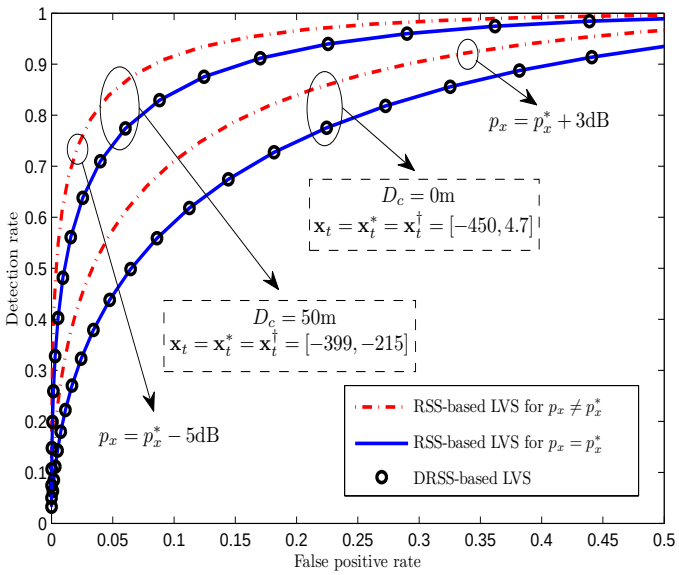

Fig. 3. ROC curves of the RSS-based LVS and the DRSS-based LVS for $\sigma_{dB} = 5$, $r = 500$m, and $N = 3$ $\big(\mathbf{x}_1 = [0, 10]$, $\mathbf{x}_2 = [131.4, -9.3]$, and $\mathbf{x}_3 = [20.6, -0.9]\big)$.

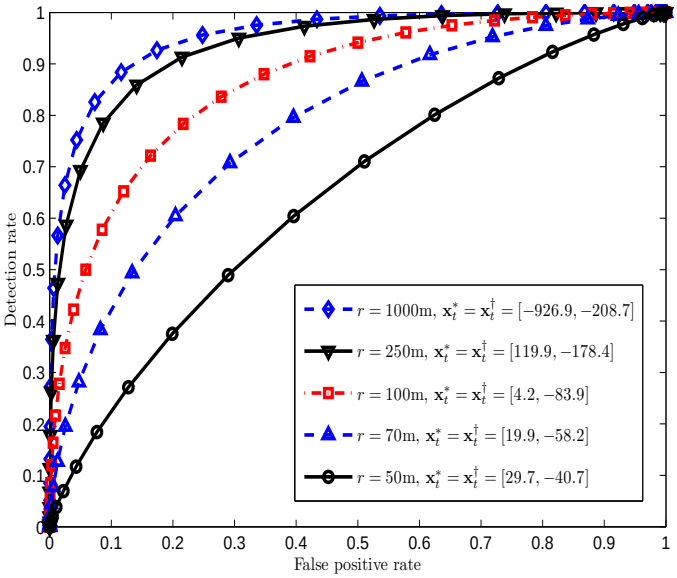

Fig. 5. ROC curves of the RSS-based LVS ($p_x = p_x^*$) and the DRSS-based LVS for $\sigma_{dB} = 5$, $D_c = 50$m, $\mathbf{x}_t = \mathbf{x}_t^* = \mathbf{x}_t^\dagger$, and $N = 3$ $\big(\mathbf{x}_1 = [0, 10]$, $\mathbf{x}_2 = [131.4, -9.3]$, and $\mathbf{x}_3 = [20.6, -0.9]\big)$.

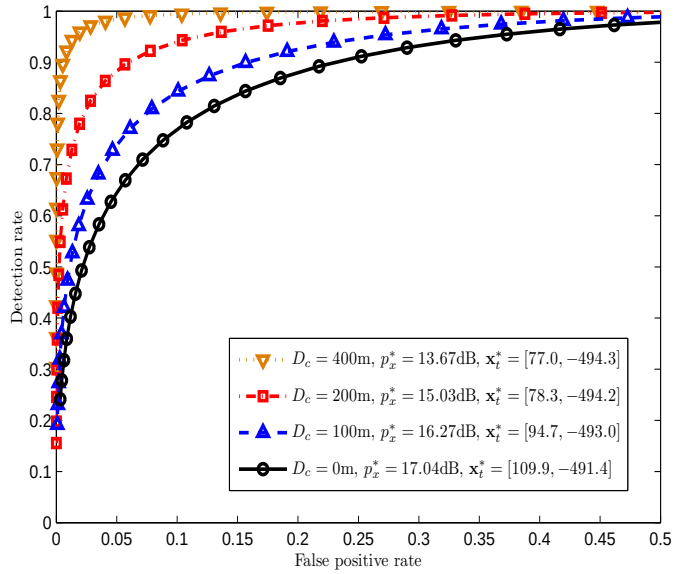

Fig. 4. ROC curves of the RSS-based LVS for $\sigma_{dB} = 7.5$, $r = 500$m, $p_x = p_x^*$, $\mathbf{x}_t = \mathbf{x}_t^*$, and $N = 3$ $\big(\mathbf{x}_1 = [-250, 10]$, $\mathbf{x}_2 = [0, -10]$, and $\mathbf{x}_3 = [250, 10]\big)$.

$p_x \neq p_x^o(\mathbf{x}_t)$ dominate the ROC curves of the DRSS-based LVS. This observation confirms that if the malicious user does not optimize his transmit power, the RSS-based LVS achieves a better performance than the DRSS-based LVS, which is provided in Corollary 5. This indicates that the RSS-based LVS is subjectively better than the DRSS-based LVS since the performance of the DRSS-based LVS is independent of the malicious user's transmit power and the determination of the optimal transmit power for the malicious user is no longer required in the DRSS-based LVS.

In Fig. 4, we investigate the impact of the spatial correlation of the shadowing on the performance of the RSS-based LVS and the DRSS-based LVS, where $D_c = 0$m corresponds to the case with uncorrelated shadowing. In Fig. 4, we set $p_x = p_x^*$ and $\mathbf{x}_t = \mathbf{x}_t^*$ for the RSS-based LVS. From (12) and (17), we can see that both p_x^* and $\mathbf{x}_t^*$ are dependent on the spatial correlation of the shadowing (they are both functions of D_c), and the exact values of p_x^* and $\mathbf{x}_t^*$ corresponding to each D_c are also provided in Fig. 4. In this figure, we first observe the ROC curve moves toward the upper left corner (i.e., the area under the ROC curve increases) as D_c increases, which shows that the performance of the RSS-based LVS becomes better as D_c increases. This observation demonstrates that the spatial correlation of the shadowing improves the detection performance of the RSS-based LVS. Intuitively, this improvement is due to the fact that the increased D_c reduces the randomness embedded in the RSS observations, and thus it is more difficult for the malicious user to mimic the legitimate observations for the increased D_c (i.e., the KL divergence presented in (10) increases as D_c increases under the system settings of Fig. 4). We note that the above performance improvement due to the spatial correlation of the shadowing is only achieved under the condition $p_x = p_x^*$ and $\mathbf{x}_t = \mathbf{x}_t^*$. If the malicious user is physically limited at some specific location $\mathbf{x}_t$ and he optimizes his transmit power as per $\mathbf{x}_t$, i.e., $p_x = p_x^o(\mathbf{x}_t)$, the spatial correlation of the shadowing does not have a monotonic impact on the performance of the RSS-based LVS. As per Theorem 3 and Corollary 6, the ROC curves provided in Fig. 4 are also valid for the DRSS-based LVS, in which we have to set $\mathbf{x}_t = \mathbf{x}_t^\dagger$. As such, we can conclude that the spatial correlation of the shadowing also improves the detection performance of the DRSS-based LVS. Also, for a determined $\mathbf{x}_t$ the spatial correlation does not have a monotonic impact on the performance of the DRSS-based LVS.

In Fig. 5, we examine the impact of the parameter r on the performance of both the RSS-based LVS and the DRSS-based LVS. We note that r is the minimum distance between the claimed location and the malicious user's true location. As such, the disc determined by $\mathbf{x}_c$ and r can be interpreted as the area protected by some physical boundaries. In Fig. 5, we observe that the ROC curve moves toward the upper left corner as r increases, which indicates that the malicious user will be easier to detect if he is further away from his claimed location. We also observe that the performance improvement due to increasing r is not significant when r is larger than some specific value (e.g., $r > 250$m).

VI. Discussions

We would like to clarify that the *a priori* knowledge model given in (1) does not represent an exhaustive decision space and also does not involve localization errors (e.g., GPS errors) on the true location of the legitimate user. However, we can adopt a generalized *a priori* knowledge model to address these two effects, which is given by

$$\begin{cases} \mathcal{H}_0: \ \mathbf{x}_t = \mathbf{x}_c + \mathbf{x}_e \ \text{ (legitimate user)}, \\ \mathcal{H}_1: \ \|\mathbf{x}_c - \mathbf{x}_t\| \geq r \ \text{ (malicious user)}, \end{cases} \tag{60}$$

where $\mathbf{x}_e$ is the *a priori* uncertainty of $\mathbf{x}_t$ at the legitimate user and the *a priori* distribution of $\mathbf{x}_e$ is denoted as $f(\mathbf{x}_e)$. We can specify different *a priori* knowledge on $\mathbf{x}_e$ in order to consider the exhaustive decision space or the localization error. Specifically, we can assume $\|\mathbf{x}_e\| < r$ for the exhaustive decision space in order to avoid any overlap between the possible spaces under $\mathcal{H}_0$ and $\mathcal{H}_1$. We would like to clarify that $\|\mathbf{x}_e\| < r$ means that $\mathbf{x}_e$ is randomly distributed inside a disk with the origin at the center and r as the radius. In practice, this disk can be approximated as an area with some physical boundaries (e.g., fences). We note that the assumption, $\|\mathbf{x}_e\| < r$, is normally adopted in the "in-region" location verification systems [41, 42], which were mainly investigated via new protocol designs rather than via statistical analysis. From a statistical point of view, we have to adopt some specific *a priori* distribution for $\mathbf{x}_e$ under the constraint $\|\mathbf{x}_e\| < r$ in order to conduct further analysis. With regard to the impact of the localization error on the true location of the legitimate user, it is reasonable to assume that $\mathbf{x}_e$ follows a zero-mean normal distribution with a covariance matrix determined by the localization error (i.e., $f(\mathbf{x}_e) = \mathcal{N}(\mathbf{0}, \mathbf{\Sigma})$, where $\mathbf{\Sigma}$ is the covariance matrix associated with the localization error). We note that the assumption of normal distribution does not ensure $\|\mathbf{x}_e\| < r$. We have checked numerically that this assumption does not significantly impact the results compared to the scenarios where $\|\mathbf{x}_e\| < r$ is actually imposed as an additional constraint.

The main variation on our RSS-based and DRSS-based LVSs caused by the adoption of the generalized *a priori* knowledge model given in (60) involves the determination of the likelihood functions under $\mathcal{H}_0$. Different from (5), in the RSS-based LVS the new likelihood function under $\mathcal{H}_0$ based on (60) is given by

$$f_g(\mathbf{y}|\mathcal{H}_0) = \int_{\mathbf{x}_e} f(\mathbf{y}|\mathbf{x}_e, \mathcal{H}_0) f(\mathbf{x}_e) d\mathbf{x}_e, \tag{61}$$

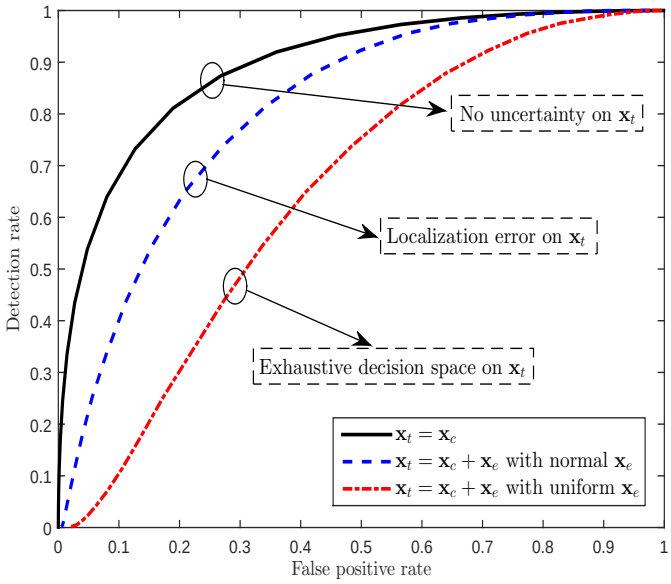

Fig. 6. ROC curves of the RSS-based LVS for $\sigma_{dB} = 5$, $r = 100$m, $\mathbf{x}_t^* = [4.2, -83.9]$, $D_c = 50$, $\mathbf{\Sigma} = diag\{\sigma_1^2, \sigma_2^2\}$, $\sigma_1 = \sigma_2 = 20$, and $N = 3$ ($\mathbf{x}_1 = [0, 10]$, $\mathbf{x}_2 = [131.4, -9.3]$, and $\mathbf{x}_3 = [20.6, -0.9]$)

where $f(\mathbf{y}|\mathbf{x}_e, \mathcal{H}_0)$ can be obtained by replacing $\mathbf{x}_c$ with $\mathbf{x}_t$ in (5). Likewise, in the DRSS-based LVS the new likelihood function under $\mathcal{H}_0$ based on (60) is given by

$$f_g(\mathbf{\Delta y}|\mathcal{H}_0) = \int_{\mathbf{x}_e} f(\mathbf{\Delta y}|\mathbf{x}_e, \mathcal{H}_0) f(\mathbf{x}_e) d\mathbf{x}_e, \tag{62}$$

where $f(\mathbf{\Delta y}|\mathbf{x}_e, \mathcal{H}_0)$ can be obtained by replacing $\mathbf{x}_c$ with $\mathbf{x}_t$ in (40). Closed-from expressions for $f_g(\mathbf{y}|\mathcal{H}_0)$ and $f_g(\mathbf{\Delta y}|\mathcal{H}_0)$ are generally hard, if not impossible, to achieve. Therefore, we numerically calculate $f_g(\mathbf{y}|\mathcal{H}_0)$ and $f_g(\mathbf{\Delta y}|\mathcal{H}_0)$, and then evaluate the performances of the resultant RSS-based and DRSS-based LVSs by utilizing our previous theoretic analysis as the benchmark.

The results of our numerical studies are provided in Fig. 6, where we adopt the RSS-based LVS as an example (following Theorem 3 the results are valid for the DRSS-based LVS as well). We note that the curve for $\mathbf{x}_t = \mathbf{x}_c$ is for the a priori model given in (1), which is obtained from our previous analysis (i.e., (32) and (33)). The curve for $\mathbf{x}_t = \mathbf{x}_c + \mathbf{x}_e$ with normal $\mathbf{x}_e$ is obtained by numerically calculating $f_g(\mathbf{y}|\mathcal{H}_0)$ given in (61) with $f(\mathbf{x}_e) = \mathcal{N}(\mathbf{0}, \mathbf{\Sigma})$, and the curve for $\mathbf{x}_t = \mathbf{x}_c + \mathbf{x}_e$ with uniform $\mathbf{x}_e$ is achieved through numerically evaluating $f_g(\mathbf{y}|\mathcal{H}_0)$ by assuming $\mathbf{x}_e$ is uniformly distributed within the region determined by r. We refer to former case as the 'localization error' and the latter as the 'exhaustive decision space'. As expected, we observe that both the localization error and the exhaustive decision space reduce the detection performance of the RSS-based LVS. We also observe that the impact of the localization error is relatively weak even when the localization error is up to tens of meters (i.e., $\sigma_1 = \sigma_2 = 20$). Meanwhile, the effect of the exhaustive decision space is significant as a consequence of the adopted uniform distribution for $\mathbf{x}_e$. This is due to the fact that the possible true locations of the legitimate user are more

concentrated near the origin under the normal distribution relative to the uniform distribution.

We would like to highlight that σ_{dB} can be estimated in our LVSs simultaneously when the *a priori* estimate is unavailable (e.g., due to time or resource limitations). When σ_{dB} is unknown, instead of utilizing the LRT given in (9) as the decision rule, we have to adopt the generalized LRT (GLRT) as our decision rule in which we have to estimate σ_{dB} based on measurements. As an example, we detail the estimation of σ_{dB} under $\mathcal{H}_0$ in the RSS-based LVS. Following (5), the likelihood function of $\mathbf{y}$ under $\mathcal{H}_0$ for a given σ_{dB} can be rewritten as

$$f\left(\mathbf{y}|\mathcal{H}_0\right)=\frac{\exp\left(-\frac{1}{2\sigma_{dB}^2}(\mathbf{y}-\mathbf{u})^T\mathbf{T}^{-1}(\mathbf{y}-\mathbf{u})\right)}{\sqrt{(2\pi)^N\sigma_{dB}^{2N}|\mathbf{T}|}}, \quad (63)$$

where $\mathbf{T}_{ij}=\left(-\frac{d_{ij}}{D_c}\ln 2\right)$. Adopting the maximum likelihood estimation, the estimate of σ_{dB} under $\mathcal{H}_0$ can be obtained through

$$\widehat{\sigma}_{dB}|\mathcal{H}_0=\underset{\sigma_{dB}}{\operatorname{argmax}}\, f\left(\mathbf{y}|\sigma_{dB},\mathcal{H}_0\right)=\sqrt{\frac{1}{N}(\mathbf{y}-\mathbf{u})^T\mathbf{T}^{-1}(\mathbf{y}-\mathbf{u})} \quad (64)$$

We note that the estimate of σ_{dB} under $\mathcal{H}_1$, $\widehat{\sigma}_{dB}|\mathcal{H}_1$, can be obtained in a similar procedure. After plugging $\widehat{\sigma}_{dB}|\mathcal{H}_0$ and $\widehat{\sigma}_{dB}|\mathcal{H}_1$ into $f\left(\mathbf{y}|\mathcal{H}_0\right)$ and $f\left(\mathbf{y}|p_x^*,\mathbf{x}_t^*,\mathcal{H}_1\right)$, respectively, we can still utilize (31) as our decision rule. However, we would like to highlight that the false positive and detection rates of (31) with $\widehat{\sigma}_{dB}|\mathcal{H}_0$ and $\widehat{\sigma}_{dB}|\mathcal{H}_1$ cannot be derived in closed-form expressions, since $\widehat{\sigma}_{dB}|\mathcal{H}_0$ and $\widehat{\sigma}_{dB}|\mathcal{H}_1$ are not equal.

VII. Conclusion

In this work we have formally analyzed for the first time, the performances of two important types of LVSs (RSS and DRSS-based) in the regime of spatially correlated shadowing. Our analysis illustrates that for anticipated levels of correlated shadowing both types of LVSs will have much improved performance. In addition, we formally proved that in fact a DRSS-based LVS has identical performance to that of an RSS-based LVS, for all levels of correlated shadowing. Even more surprisingly, the identical performance of RSS and DRSS-based LVSs was found to hold even when the adversary cannot optimize his true location. We found the performance of an RSS-based LVS to be better than that of a DRSS-based LVS only in the case where the adversary cannot optimize *all* variables under her control. The results presented here will be important for a wide range of practical location authentication systems deployed in support of emerging wireless network applications.

Acknowledgments

This work was funded by Australian Research Council Grants DP120102607 and DP150103905. We thank the Editor and the anonymous referees for their valuable comments.

References

[1] R. A. Malaney, "A location enabled wireless security system," in *Proc. IEEE GlobeCOM*, Nov. 2004, pp. 2196–2200.
[2] A. Vora, M. Nesterenko, "Secure location verification using radio broadcast," *IEEE Trans. on Dependable and Secure Computing*, vol. 3, no. 4, pp. 377–385, Oct. 2006.
[3] R. A. Malaney, "Securing Wi-Fi networks with position verification," *International J. Sec, Net.*, vol. 2, pp. 27–36, Mar. 2007.
[4] S. Čapkun, K. B. Rasmussen, M. Čagalj, and M. Srivastava, "Secure location verification with hidden and mobile base station," *IEEE Trans. Mobile Comput.*, vol. 7, no. 4, pp. 470–483, Apr. 2008.
[5] Y. Sheng, K. Tan, G. Chen, D. Kotz, and A. Campbell, "Detecting 802.11 MAC-layer spoofing using received signal strength," in *Proc. IEE INFOCOM*, Apr. 2008, pp. 1768–1776.
[6] Y. Chen, J. Yang, W. Trappe, and R. P. Martin, "Detecting and localizing identity-based attacks in wireless and sensor networks," *IEEE Trans. Veh. Technol.*, vol. 59, no. 5, pp. 2418–2434, Jun. 2010.
[7] R. Zekavat and R. Buehrer, "Handbook of Position Location: Theory, Practice and Advances," vol. 27. Wiley-IEEE Press, 2012.
[8] J. T. Chiang, J. J. Haas, J. Choi, and Y. Hu "Secure location verification using simultaneous multilateration," *IEEE Trans. Wireless Commun.*, vol. 11, no. 2, pp. 584–591, Feb. 2012.
[9] S. Yan, R. Malaney, I. Nevat, and G. Peters, "An information theoretic location verification system for wireless networks," in *Proc. IEEE GlobeCOM*, Dec. 2012, pp. 5415–5420.
[10] S. Yan, R. Malaney, I. Nevat, and G. Peters, "Optimal information-theoretic wireless location verification," *IEEE Trans. Veh. Technol.*, vol. 63, no. 7, pp. 3410–3422, Sep. 2014.
[11] T. Leinmüller, E. Schoch, F. Kargl, and C. Maihöfer, "Influence of falsified position data on geographic ad-hoc routing," in *Proceedings of the second European Workshop on Security and Privacy in Ad hoc and Sensor Networks (ESAS)*, Jul. 2005, pp. 102–112.
[12] T. Leinmüller and E. Schoch, "Greedy routing in highway scenarios: the impact of position faking nodes," in *Proc. WIT*, 2006.
[13] M. Al-Rabayah and R. Malaney, "A new scalable hybrid routing protocol for VANETs," *IEEE Trans. Veh. Technol.*, vol. 61, no. 6, pp. 2625–2635, Jul. 2012.
[14] S. Chen, Y. Zhang, and W. Trappe, "Inverting sensor networks and actuating the environment for spatio-temporal access control" in *Proceedings of the fourth ACM workshop on Security of ad hoc and sensor networks*, Oct. 2006, pp. 1–12.
[15] S. Capkun, M. Cagalj, G. Karame, and N.O. Tippenhauer, "Integrity regions: authentication through presence in wireless networks", *IEEE Trans. Mob. Comput.*, vol. 9, no. 11, pp. 1608–1621, Nov. 2010.
[16] F. Liu and X. Cheng, "LKE: A self-configuring scheme for location-aware key establishment in wireless sensor networks," *IEEE Trans. Wireless Commun.*, vol. 7, no. 1, pp. 224–232, Jan. 2008.
[17] S. Yan, R. Malaney, I. Nevat, and G. Peters, "Signal strength based location verification under spatially correlated shadowing," in *Proc. IEEE ICC*, Jun. 2014, pp. 2617–2623.
[18] G. Yan, S. Olariu, and M. Weigle, "Providing location security in vehicular ad hoc networks," *IEEE Wireless Commun.*, vol. 16, no. 6, pp. 48-55, Dec. 2009.
[19] G. Wang and K. Yang, "A new approach to sensor node localization using RSS measurements in wireless sensor networks," *IEEE Trans. Wireless Commun.*, vol. 10, no. 5, pp. 1389–1395, May 2011.
[20] J. Gu, S. Chen, and T. Sun, "Localization with incompletely paired data in complex wireless sensor network," *IEEE Trans. Wireless Commun.*, vol. 10, no. 9, pp. 2841–2849, Sep. 2011.
[21] F. Montorsi, F. Pancaldi, and G. M. Vitetta, "Map-aware models for indoor wireless localization systems: an experimental study," *IEEE Trans. Wireless Commun.*, vol. 13, no. 5, pp. 2850–2862, May 2014.
[22] R. Malaney, "Nuisance parameters and location accuracy in log-normal fading models," *IEEE Trans. Wireless Commun.*, vol. 6, no. 3, pp. 937–947, Mar. 2007.
[23] J. Wang, J. Chen, and D. Cabric, "Cramer-rao bounds for joint RSS/DoA-based primary-user localization in cognitive radio networks," *IEEE Trans. Wireless Commun.*, vol. 12, no. 3, pp. 1363–1375, Mar. 2013.
[24] M. Gudmundson, "Correlation model for shadow fading in mobile radio systems," *Electron. Lett.*, vol. 27, no. 23, pp. 2145–2146, Aug. 1991.
[25] J. C. Liberti and T. S. Rappaport, "Statistics of shadowing in indoor radio channels at 900 and 1900 MHz," in *Proc. IEEE MILCOM*, Oct. 1992, pp. 1066–1070.
[26] K. Zayana and B. Guisnet, "Measurements and modelisation of shadowing cross-correlations between two base-stations," in *Proc. IEEE ICUPC*, Oct. 1998, pp. 101–105.

[27] N. Patwari and P. Agrawal, "Effects of correlated shadowing; Connectivity, localization, and RF tomography," in *Proc. IEEE IPSN*, Apr. 2008, pp. 82–93.
[28] P. Agrawal and N. Patwari, "Correlated link shadow fading in multihop wireless networks," *IEEE Trans. Wireless Commun.*, vol. 8, no. 8, pp. 4024–4036, Aug. 2009.
[29] R. M. Vaghefi and R. M. Buehrer, "Received signal strength-based sensor localization in spatially correlated shadowing," in *Proc. IEEE ICASSP*, May 2013, pp. 4076–4080.
[30] J. Wang, Q. Gao, Y. Yu, P. Cheng, L. Wu, and H. Wang, "Robust device-free wireless localization based on differential RSS measurements,", *IEEE Trans. Ind. Electron.*, vol. 60, no. 12, pp. 5943–5952, Dec. 2013.
[31] P. S. Mandal and A. K. Ghosh, "A statistical approach towards secure location verification in noisy wireless channels," *Inter. J. Found. Comput. Sci*, vol. 25, no. 5, pp. 563–584, Aug. 2014.
[32] S. Yan, R. Malaney, I. Nevat, and G. Peters, "Location spoofing detection systems for VANETs by a single base station in Rician fading channels," in *Proc. IEEE VTC Spring*, May. 2015, pp. 1–6.
[33] S. Yan, R. Malaney, I. Nevat, and G. Peters, Location verification systems for VANETs in Rician fading channels, *IEEE Trans. Veh. Technol.*, accepted to appear, DOI: 10.1109/TVT.2015.2453160, Jul. 2015.
[34] J. Neyman and E. Pearson, "On the problem of the most efficient tests of statistical hypotheses," *Phil. Trans. R. Soc. A*, vol. 231, pp. 289–337, Jan. 1933.
[35] M. Barkat, *Signal Detection and Estimation*, Boston, MA: Artech House, 2005.
[36] S. Eguchi and J. Copas, "Interpreting Kullback-Leibler divergence with the Neyman-Pearson lemma," *J. Multivar. Anal.*, vol. 97, no. 9, pp. 2034–2040, Oct. 2006.
[37] S. Kullback and R. A. Leibler, "On information and sufficiency," *Annals of Mathematical Statistics*, vol. 22, no. 1, pp. 79–86, 1951.
[38] L. L. Scharf and B. Friedlander, "Matched subspace detectors," *IEEE Trans. Signal Process.*, vol. 42, no. 8, pp. 2146–2157, Aug. 1994.
[39] S. M. Kay, J.R. Gabriel, "An Invariance property of the generalized likelihood ratio test," *IEEE Signal Process. Lett.*, vol. 10, no. 12, pp. 352–355, Dec. 2003.
[40] J. Sherman and W. J. Morrison, "Adjustment of an inverse matrix corresponding to a change in one element of a given matrix," *Ann. Math. Statist.*, vol. 21, no. 1, pp. 124–127, Mar. 1950.
[41] N. Sastry, U. Shankar, and D. Wagner, "Secure verification of location claims," in *Proc. ACM WiSe*, Sep. 2003, pp. 1–10.
[42] Y. Wei and Y. Guan, "Lightweight location verification algorithms for wireless sensor networks," *IEEE Trans. Parallel Distrib. Syst.*, vol. 24, no. 5, pp. 938–950, May 2013.